57

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/882,585	06/15/2001	Christopher Bolin	2114P018	9593

7590 12/22/2005

ZILKA-KOTAB, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER
SON, LINH L D

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 12/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/882,585	BOLIN, CHRISTOPHER	
	Examiner	Art Unit	
	Linh LD Son	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 June 2001*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,5-16,19-30,33-44 and 47-56* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,5-16,19-30,33-44 and 47-56* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is responding to the Amendment received on 09/26/2005.

2. Claims 1-2, 5-16, 19-30, 33-44, and 47-56 are pending. Claims 3-4, 17-18, 31-32, and 45-46 are canceled.

Claim Objections

3. Claims 12, 26, 40, and 54 recites the term or acronym "VxD". Applicant needs to spell-out the acronym.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-2, 5, 8, 15-16, 19, 22, 29-30, 33, 36, 43-44, 47, and 50 are rejected under 35 U.S.C. 102(e) as being anticipated by Hartley et al, US Publication No. 20020026591, hereinafter "Hartley".

6. As per claims 1 and 15:

Hartley teaches "A method for preventing needless rescanning of objects comprising: verifying an integrity of a file system by scanning the file system resulting in at least one known scanned region" (Para 0041); "creating a database of the known scanned regions of the verified file system" in (Para 0035, database 42); and "validating an integrity of an object in the file system against the database of known scanned regions" in (Para 0041); wherein the verifying comprises: "receiving a file system event from a real-time monitoring -system, the file system event indicating that an object in the file system has been accessed" in (Para 0041-43, and 0049); and "flagging the database of known scanned regions to indicate which of the known scanned regions was occupied by the accessed object wherein the validating utilizes the flagging" in (Para 0048, and 0068).

7. As per claims 2, 16, 30, and 44:

Hartley teaches "The method of claims 1, 15, 29, and 43, wherein verifying the integrity of the file system comprises scanning the objects in the file system for a presence of viruses" in (Para 0041).

8. As per claims 5, 19, 33, and 47:

Hartley teaches "The method of claims 1, 15, 29, and 43 wherein the database of known scanned regions comprises a copy of a partition table data structure indicating an identity and a location of a known scanned region occupied by the object" in (Para 0041).

9. As per claims 8, 22, 36, and 50:

Hartley teaches "The method of claims 7, 15, 29, 43, wherein validating the integrity of an object comprises determining that the object does not occupy a flagged known scanned region" in (Para 0048).

10. As per claim 29:

Hartley teaches "An integrity validator comprising: a verifier to verify the integrity of a file system by scanning the file system resulting in at least one known scanned region" (Para 0041); "a database of the known scanned regions of the verified file system in (Para 0035, database 42); and a validator to validate the integrity of an object in the file system against the database of known scanned regions" " in (Para 0041); "wherein the verifying comprises: receiving a file system event from a real-time monitoring system, the file system event indicating that an object in the system has been accessed" in (Para 0041-43, and 0049); and "flagging the database of known scanned re 'Dons to indicate which of the known scanned regions was occupied by the accessed object; wherein the validating utilizes the flagging" in (Para 0048, and 0068).

11. As per claim 43:

Hartley teaches "A computer system comprising: a processor coupled to a system bus; a memory coupled to the processor through the system, bus; a machine-accessible medium coupled to the processor through the system bus; an integrity process executed from the machine-accessible medium by the processor, wherein the integrity process causes the processor to verify the integrity of a file system resulting in at least one known scanned region" (Para 0028, and 0041), "to create a database of known scanned regions of the verified file system" in (Para 0035, database 42), and "to validate the integrity of an object in the file system against the database of known scanned regions" in (Para 0041); wherein the verifying comprises: "receiving a file system event from a real-time monitoring system, the file system event indicating that t an object in the file system has been accessed" in (Para 0041-43, and 0049); and "flagging the database of known scanned regions to indicate which of the known scanned regions was occupied by the accessed object; wherein the validating utilizes the flagging" in (Para 0048, and 0068).

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claims 6-7, 9-14, 20-21, 23-28, 34-35, 37-42, 48-49, and 51-56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hartley in view of Jenevein (Cited in PTO 892 dated 03/25/2005)

14. As per claims 6, 20, 34, and 48:

Hartley does not specifically teach "the partition table data structure includes an inode that contains information about the object other than name, and a directory block that contains the object name and a number of the inode of the object". Nevertheless, Jenevein teaches "The partition table data structure includes an inode that contains information about the object other than name, and a directory block that contains the object name and a number of the inode of the object" in (Col 11 lines 8-15, Col 13 line 15 to Col 14 line 27, and Col 15 lines 20-33). Therefore, it would have been obvious at the time of the invention was made for one ordinary skill in the art to incorporate the tracking of detail information about the object with Hartley's teaching of monitoring and detecting security problem with a file system.

15. As per claims 7, 21, 35, and 49:

Hartley does not specifically teach "the partition table data structure includes a super block that contains information about the file system as a whole, and a data block that contains a location in the file system where the object is stored. Nevertheless, Jenevein teaches "the partition table data structure includes a super block that contains information about the file system as a whole, and a data block that contains a location in

the file system where the object is stored" in (Col 13 line 15 to Col 14 line 27, and Col 15 lines 20-33).

Therefore, it would have been obvious at the time of the invention was made for one ordinary skill in the art to incorporate the tracking of detail information about the object with Hartley's teaching of monitoring and detecting security problem with a file system.

16. As per claims 9, 23, 37, and 51:

Hartley does not specifically teach "flagging comprises indicating which of the inodes and directory blocks were occupied by the accessed object. Nevertheless, Jenevein teaches "the flagging comprises indicating which of the inodes and directory blocks were occupied by the accessed object" in (Col 11 lines 8-15, Col 15 line 20-30, and Col 13 line 15 to Col 14 line 27). Therefore, it would have been obvious at the time of the invention was made for one ordinary skill in the art to incorporate the tracking of detail information about the object with Hartley's teaching of monitoring and detecting security problem with a file system.

17. As per claims 10, 24, 38:

Hartley does not specifically teach "wherein validating the integrity of art object comprises determining that the object does not occupy a flagged inode and directory block. Nevertheless, Jenevein teaches "validating the integrity of an object comprises determining that the object does not occupy a flagged inode and directory block" in (Col 11 lines 8-15, Col 14 line 10 to Col 15 line 10). Therefore, it would have been obvious at the time of the invention was made for one ordinary skill in the art to incorporate the

tracking of detail information about the object with Hartley's teaching of monitoring and detecting security problem with a file system.

18. As per claims 11, 25, 39, and 53:

Hartley teaches "rescanning the object when the integrity of the object hiss not been validated; and bypassing rescanning the object when the integrity of the object has been validated.

19. As per claims 12, 26, 40, and 54:

Hartley does not specifically teach "the real-time monitoring system is a VxD program". Nevertheless, Jenevein teaches "The real-time monitoring system is a VxD program" in (Col 2 lines 28-35). Therefore, it would have been obvious at the time of the invention was made for one ordinary skill in the art to modify Hartley's invention to incorporate Jenevein's VxD program (IBM Compatible program) to provide a universal solution to both IBM and Unix environment.

20. As per claims 13, 27, 41, and 55:

Hartley does not specifically teach "the real-time monitoring system is a UNIX daemon". Nevertheless, Jenevein teaches a method of configuring and monitoring a storage media in a computer system or attached to a computer network that includes "the real-time monitoring system is a UNIX daemon" in (Col 2 lines 30-39). Therefore, it would have been obvious at the time of the invention was made for one ordinary skill in the art to incorporate Jenevein's real-time monitoring system Unix daemon with

Hartley's teaching to monitor and detect a computer security problem in a Unix environment.

21. As per claims 14, 28, 42, and 56:

Hartley does not specifically teach "the real-time monitoring system is a network loadable module. Nevertheless, Jenevein does teaches "the real-time monitoring system is a network loadable module" in (Col 4 lines 15-24). Therefore, it would have been obvious at the time of the invention was made for one ordinary skill in the art to modify Hartley's invention to incorporate Jenevein's teaching to provide the monitoring service over the network.

Conclusion

22. Applicant has amended claims 1, 15, 29, and 43, which necessitated new grounds of rejection. See Rejections above.

23. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

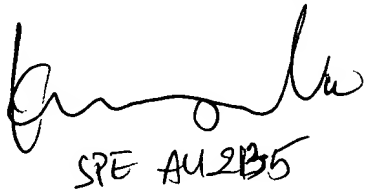
A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

24. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Linh LD Son whose telephone number is 571-272-3856. The examiner can normally be reached on 9-6 (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Linh LD Son
Examiner
Art Unit 2135